

**CERTIFICATE OF AUTHENTICITY**  
**OF DATA COPIED FROM AN ELECTRONIC DEVICE OR STORAGE MEDIA**  
**PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(14)**

I, Thorsten Lucke, attest and certify, under penalty of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct.

1. From 1996 to 2023, I have been employed as a police officer with the Philadelphia, Pennsylvania Police Department. I have been a detective since 2002, and have spent the last 17 years assigned to the Homicide Unit. I have extensive training and experience in examining and extracting data from digital devices, such as cellular telephones.

My training includes but is not limited to:

2008 – 1 Day - Federal Bureau of Investigation (FBI) Regional Computer Forensics Laboratory (RCFL): Forensic Cellular Phone Examinations (Certification with Cellebrite Universal Forensics Extraction Device (UFED), extracting, decoding, analysis and reporting of data from mobile phones.

2020 – 4 Weeks - United States Secret Service National Computer Forensics Institute (NCFI), Hoover Alabama: Mobile Device Examiner, Tools necessary to conduct, analyze and document mobile device examinations, Cellebrite Mobile Forensic Training, Cellebrite Physical Analyzer, Magnet Forensics Axiom, advanced mobile forensics techniques (JTag, Chip off, ISP).

2021 – 1 Week - United States Secret Service National Computer Forensics Institute (NCFI), Hoover Alabama: Advanced Mobile Device Examiner, Advanced mobile forensic analysis tools for cell phones, GPS units, and tablets.



2023 – 1 Week -United States Secret Service National Computer Forensics Institute (NCFI),  
Hoover Alabama: Performing repairs on damaged electronic devices, including cellular devices,  
storage media, etc, to facilitate data recovery. Replacing / repairing batteries, screens, logic  
boards, chips, charging ports and other parts.

During my law enforcement career, I examined more than three thousand (3000) digital devices.

2. I am qualified to authenticate the digital extraction referenced in this paragraph  
because of my experience and training and because I created the digital reports listed below:

Original Device	Source	Date of Image
Device #1 Apple iPhone 12, IMEI: 353044116123382	Neil Satterwhite (Philadelphia Police Dept. Case # 21-03- 032966, Control # S21- 101)	7/27/2021
Device #2 Apple iPhone 12, IMEI: 353042116210316	Neil Satterwhite (Philadelphia Police Dept. Case # 21-03- 032966, Control # S21- 101)	7/27/2021

3. The reports described above are a true representation of the data recovered from the  
devices (cellular telephones). Both of the devices (Apple iPhones) were locked at the  
time of the examination, each requiring an unknown 4-digit Pin type passcode.  
Neither device were at the time and still are not supported for a brute force  
(unlocking) process by the current forensic extraction tool(s). Two different types of  
levels extractions were obtained from the two devices. A partial AFU (After First

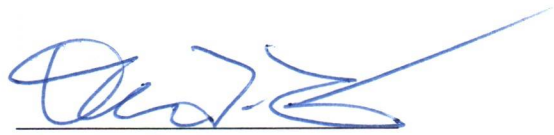
Unlock) extraction was obtained from Device #1. This is an extraction level providing data close to what a Full File System type extraction would obtain from an unlocked device. A partial BFU (Before First Unlock) extraction was obtained from Device #2. This is a much more limited type of extraction. Both types of extractions obtained for the respective devices were the most extensive extractions obtainable from each device with their respective device model, Operating System (OS), and encryption level combinations.

4. The reports listed above were made at or near the time the content from the digital devices were seized using specialized forensic tool, called Graykey. The recovered data was then processed and rendered utilizing another specialized forensic software called Cellebrite Physical Analyzer. In my training and experience, this forensic software creates an accurate and reliable report of data recovered from digital mobile devices at the moment in time in which the extraction is performed, and I have regularly relied on Cellebrite to create an accurate and reliable extraction in the past.

5. Furthermore, I know that the forensic report rendering process was complete and accurate because the forensic software generated a hash (i.e., digital fingerprint) of the extracted data and because the software expressly indicated that the extraction / rendering was successful.

I further state that this certification is intended to satisfy Rules 902(11) and 902(14) of the Federal Rules of Evidence.

09/19/23  
Date

  
Thorsten Lucke  
Detective, Philadelphia Police Dept.